

[NT] Trend Micro ServerProtect Multiple Vulnerabilities (EarthAgent)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-12/msg00072.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 22 Dec 2005 12:44:22 +0200
-

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>
-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.
<http://www.securiteam.com/maillinglist.html>

Trend Micro ServerProtect Multiple Vulnerabilities (EarthAgent)

SUMMARY

"

<<http://www.trendmicro.com/en/products/file-server/sp/evaluate/overview.htm>> ServerProtect provides comprehensive antivirus scanning for servers, detecting and removing viruses from files and compressed files in real time — before they reach the end user."

Improper packet handling allows attackers to cause a DoS with Trend Micro ServerProtect EarthAgent making 100% CPU resource. In addition, the use of old MFC library and the Management Console tool of Trend Micro ServerProtect allows attackers to execute arbitrary code with the privileges of the underlying web server and to view content of arbitrary files on the system with ServerProtect Management Console.

DETAILS

Vulnerable Systems:

- * Trend Micro ServerProtect for Windows Management Console version 5.58 running with Trend Micro Control Manager 2.5/3.0 and Trend Micro Damage Cleanup Server 1.1.
- * Microsoft Visual Studio version 6.0

[NT] Trend Micro ServerProtect Multiple Vulnerabilities (EarthAgent)

Immune Systems:

* Microsoft Visual Studio version 6.0 SP6

EarthAgent Remote DoS:

The problem specifically exists within ServerProtect EarthAgent in the handling of maliciously crafted packets transmitted with the magic value "\x21\x43\x65\x87" targeting TCP port 5005. A memory leak also occurs with each received exploit packet allowing an attacker to exhaust all available memory resources with repeated attack.

Successful exploitation of the described vulnerability allows unauthenticated remote attackers to consume 100% CPU resources, increasingly consume memory resources and potentially crash the underlying operating system. Full CPU utilization can be achieved with a single packet, memory consumption occurs incrementally on subsequent attacks.

Vendor Status:

The vendor has issued a patch fixing the problem: "Contact Trend Micro Technical Support to request for the SPNT5.58_HotfixB1137.zip file, which should only be installed on servers running SPNT 5.58."

ServerProtect relay.dll Chunked Overflow:

The problem specifically exists within the relay.dll ISAPI application upon processing of large POST requests with "wrapped" length values, because of the use of an old MFC library.

Example:

```
POST /TVCS/relay.dll HTTP/1.0
```

```
Transfer-Encoding: chunked
```

```
80000000
```

```
[ 50,000 bytes or so ]
```

The above example request will create an exploitable heap corruption providing the attacker with a near arbitrary 4-byte overwrite. By overwriting the address of a soon to be called function the attacker can seize CPU control and eventually execute arbitrary code.

Successful exploitation of the described issue allows remote attackers to execute arbitrary code with the privileges of the underlying web server. Exploitation does not require credentials, thereby exacerbating the impact of this vulnerability.

isaNVWRequest.dll Chunked Overflow:

The problem specifically exists within the isaNVWRequest.dll ISAPI application upon processing of large POST requests with "wrapped" length values, example:

```
POST /ControlManager/cgi-bin/VA/isaNVWRequest.dll HTTP/1.0
```

```
Transfer-Encoding: chunked
```

[NT] Trend Micro ServerProtect Multiple Vulnerabilities (EarthAgent)

80000000
[50,000 bytes or so]

This example request will create an exploitable heap corruption providing the attacker with a near arbitrary 4-byte overwrite. By overwriting the address of a soon to be called function, the attacker can seize CPU control and eventually execute arbitrary code.

Successful exploitation of the described issue allows remote attackers to execute arbitrary code with the privileges of the underlying web server. Exploitation does not require credentials, thereby exacerbating the impact of this vulnerability.

Vendor Status:

The response for both relay.dll Chunked Overflow and isaNVWRequest.dll Chunked Overflow is:

"Trend Micro has recently become aware of a vulnerability related to the Microsoft Foundation Classes (MFC) static libraries used by Trend Micro products to create Internet Server Application Programming Interface (ISAPI) programs for IIS user interfaces. Under certain heavy load conditions, the MFC ISAPI produces invalid arguments, which can create an access violation, and thus a denial of service to users. The original MFC vulnerability was reported and patched in 2002 by Microsoft, however, in April 2005, Microsoft published new solutions, and vendors were required to rebuild programs to link to the new library. During this transition period, manual solutions are available through Trend Micro technical support for customers wishing to take precautionary measures, in the unlikely event of an exploit targeted at the MFC vulnerability.

The potential impact to Trend Micro products is limited to some versions of InterScan eManager, InterScan Web Protect, OfficeScan, and Control Manager. Many of these products will be updated in the next version release.

For now, use the workarounds provided:

Option I: Use the Microsoft URLScan Tool

1. Download any of the following:

Note: The tool prevents a potential thread by rejecting the specified requests.

- * URLScan 2.5 (for IIS 6.0)
- * IIS Lockdown Tool 2.1 (for IIS 4.0 or 5.0)

2. Run the URLScan tool. The urlscan folder is automatically created in the C:\WINDOWS\system32\inetrv\urlscan directory.

3. Open Windows Explorer and go to the C:\WINDOWS\system32\inetrv\urlscan directory.

[NT] Trend Micro ServerProtect Multiple Vulnerabilities (EarthAgent)

4. Find the URLScan.ini file and open with a text editor like Notepad.
5. Find the [AllowExtensions] section and add the following file extensions:

- * .exe
- * .ini
- * .dat
- * .asp

6. Find the [DenyHeaders] section and add the transfer-encoding: parameter.
7. Find the [Options] section and change the value of UseAllowExtensions to "0".
8. Under [DenyExtensions], remove the following file extensions:
 - * .exe
 - * .ini
 - * .dat
 - * .asp

9. Save the changes and close the file.
10. Stop and start the Web service.

Option II: Change build environments

Trend Micro recommends changing the build environments to Visual C++ 6.0 with Service Pack 6."

ServerProtect Crystal Reports ReportServer File Disclosure:

The problem specifically exists within the handling of the IMAGE parameter in the script rptserver.asp. The vulnerable area of code is outlined in the following snippet:

```
Set session("oEMF") = Server.CreateObject("CREmfgen.CREmfgen.2")
Call ParseQS()
if IMAGE <> "" then
Call session("oEMF").StreamImage(IMAGE, DEL)
Response.End
end if
```

An attacker can utilize directory traversal modifiers to traverse outside the system temporary directory and access any file on the same volume.

Successful exploitation of the described vulnerability allows remote attackers to view the contents of arbitrary files on the underlying system. Exploitation does not require credentials thereby exacerbating the impact of this vulnerability.

Vendor Status:

"Trend Micro has become aware of a vulnerability related to Crystal Report, a reporting component found in Trend Micro Control Manager (v2.5 and v3.0). Under certain conditions, arbitrary files on the ReportServer

[NT] Trend Micro ServerProtect Multiple Vulnerabilities (EarthAgent)

volume inside Trend Micro Control Manager software could be viewed or accessed remotely. Trend Micro is currently consulting with Crystal Report regarding permanent solutions to this reporting component. A temporary workaround solution can be recommended through contacting Trend Micro customer and technical support."

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-1928>>
CVE-2005-1928
<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-1929>>
CVE-2005-1929
<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-1930>>
CVE-2005-1930

Disclosure Timeline:

06/03/2005 – Initial vendor notification
06/05/2005 – Initial vendor response
12/14/2005 – Public disclosure

ADDITIONAL INFORMATION

The information has been provided by iDefense.

The original article can be found at:

<<http://www.odefense.com/application/poi/display?id=352&type=vulnerabilities>>
<http://www.odefense.com/application/poi/display?id=352&type=vulnerabilities>,

<<http://www.odefense.com/application/poi/display?id=353&type=vulnerabilities>>
<http://www.odefense.com/application/poi/display?id=353&type=vulnerabilities>,

<<http://www.odefense.com/application/poi/display?id=354&type=vulnerabilities>>
<http://www.odefense.com/application/poi/display?id=354&type=vulnerabilities>,

<<http://www.odefense.com/application/poi/display?id=356&type=vulnerabilities>>
<http://www.odefense.com/application/poi/display?id=356&type=vulnerabilities>

The MFC advisory can be found at:

<<http://www.securiteam.com/windowsntfocus/5TP0J0K7PE.html>>
<http://www.securiteam.com/windowsntfocus/5TP0J0K7PE.html>

The Vendor advisory can be found at:

<<http://kb.trendmicro.com/solutions/search/main/search/solutionDetail.asp?solutionID=25254>>
<http://kb.trendmicro.com/solutions/search/main/search/solutionDetail.asp?solutionID=25254>

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@xxxxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxx

=====
=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.

-
- Prev by Date: [*\[NT\] Internet Explorer Multiple Download Dialog Vulnerabilities \(MS05-054\)*](#)
 - Next by Date: [*\[EXPL\] Macromedia Flash Media Server DoS \(Exploit, Single Character\)*](#)
 - Previous by thread: [*\[NT\] Internet Explorer Multiple Download Dialog Vulnerabilities \(MS05-054\)*](#)
 - Next by thread: [*\[EXPL\] Macromedia Flash Media Server DoS \(Exploit, Single Character\)*](#)
 - Index(es):
 - ◆ [*Date*](#)
 - ◆ [*Thread*](#)